REMARKS

Claims 1-4, 6, 8-21, 23, 25-38, 40, and 42-51 are pending.

In the present Office Action, claims 1-2, 6, 8, 10, 12, 15-16, 18-19, 23, 25, 27, 29, 32-33, 35-36, 40, 42, 44, 46, and 49-50 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Bots, U.S. Patent No. 6,226,748 (hereinafter "Bots"). Applicant submits that the claims recite features and limitations not suggested or taught by the cited art. Applicant respectfully traverses the above rejections and requests reconsideration in view of the following discussion.

In the present Office Action, the examiner cites the virtual private network (VPN) of Bots as being equivalent to the recited firewall. In the Response dated June 2, 2006, Applicant pointed out distinctions between the recited firewall and the VPN of Bots. On page 7 of the present Office Action, the examiner states:

> "Bots implements a unique firewall comprising Virtual Private Network Units (VPNUs). . . . the two VPNUs are acting as part of a single firewall entity."

However, not only does the Applicant disagree with the assertion that the cited virtual private network is equivalent to the recited firewall, but even the Bots reference itself disagrees with such an equation. In particular, Bots teaches:

> "The overall architecture of the present invention is robust. It allows end users the convenience of proprietary data communications to take place over a public network space such as the Internet. The architecture of the present invention also allows a wide variety of compression, encryption and authentication technologies to be implemented, so long as the VPN units at each end of the transaction support the associated protocols. The present invention is also capable

> of working in concert with traditional Internet security mechanisms such as corporate firewalls. A firewall might operate in series with the VPN unit at a given site, or, intelligently be configured in a single box with the VPN unit to provide parallel firewall and VPN unit security functions." (Bots, col. 9, lines 13-25).

Accordingly, Applicant disagrees with the suggested equivalence between Bots VPN and the recited firewall, and Bots also disagrees with the suggested equivalence. Therefore, Applicant submits the cited virtual private network is not equivalent to the recited firewall as suggested, and the node as recited in the present application is not equivalent to Bots virtual private network.

In addition to the above, Applicant previously noted that Bots does not disclose "changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS." The examiner cited col. 7, lines 1-19 of Bots as disclosing these features. However, Applicant disagrees. The cited portion of Bots is as follows:

> "At decision box 320, it is determined whether or not the source and destination addresses for the data packet are both members of the same VPN group. This determination may be made with reference to lookup tables that are maintained by the VPN units or reference to other memory mechanisms. This step may be thought of as member filtering for data packets being transmitted between the particular site and the VPN unit which services it. If the source and destination address for the data packet are not both members of the same VPN group, then at step 330 the packet is forwarded to the Internet as ordinary Internet traffic from the site as though the VPNU were not involved. In which case, the procedure ends at step 335. In one alternative embodiment, it may be desirable to discard data traffic that is not destined between members of a VPN group rather than forwarding it as unsecure traffic. In another alternative embodiment, it may be desirable to provide the option to either pass or discard non-VPN-group data traffic."

Applicant submits the above disclosure of Bots is clearly not equivalent to "changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS." Rather, this disclosure of Bots merely teaches that if a source and destination address for a packet are not both members of a same VPN group, the packet may be forwarded as ordinary Internet traffic (or discarded). Applicant sees nothing concerning a rule which teaches changing an incoming PCS to an outgoing PCS in response to determining the first incoming PCS matches the second incoming PCS.

In addition, claim 1 recites three comparisons: detecting said first incoming PCS is not a subset of an interface community set (IFCS) of said interface, comparing said first incoming PCS to a second incoming PCS specified by the first rule, and comparing said outgoing PCS with a destination community set of said first data packet. Bots fails to teach or suggest all three comparisons. In contrast to the above claimed features, Bots discloses:

> "At decision box 320, it is determined whether or not the source and destination addresses for the data packet are both members of the same VPN group. This determination may be made with reference to lookup tables that are maintained by the VPN units or reference to other memory mechanisms. This step may be thought of as member filtering for data packets being transmitted between the particular site and the VPN unit which services it." (Bots, Col. 7, lines 1-9).
>
> "At decision box 420, the inbound data packet is examined to determine if the source and destination addresses of the data packet are both members of the same VPN group. It is assumed that the lookup tables maintained by all of the VPN units are both consistent and coherent." (Bots, Col. 7, lines 60-65).

As may be seen from the above, Bots' method looks up the VPN group of the source address and the VPN group of the destination address and compares them to see if the two groups are the same. These steps are performed in both the transmitting VPNU and the receiving VPNU. Hence, Bots discloses, at most, two comparisons. Furthermore, the three comparisons recited in claim 1 involve a first incoming PCS and

an (IFCS), a first incoming PCS and a second incoming PCS, and an outgoing PCS and a destination community set. No two of these comparisons involve the same two community sets. Accordingly, Applicant submits that Bots fails to disclose all of the comparisons recited in claim 1.

For at least the above reasons, Applicant submits that each of the independent claims are patentably distinguishable over the cited art. Applicant's comments in the Response dated June 2, 2006, are not repeated herein, but are applicable and are incorporated by reference.

Applicant believes the application to be in condition for allowance. However, should the examiner believe otherwise, the below signed representative requests a telephone interview (512) 853-8866 in order to facilitate a speedy resolution.

CONCLUSION

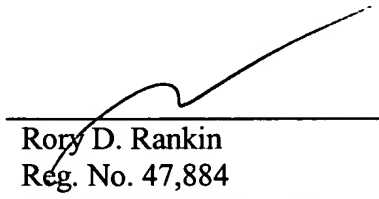
Applicant submits the application is in condition for allowance, and an early notice to that effect is requested.

If any extensions of time (under 37 C.F.R. § 1.136) are necessary to prevent the above referenced application(s) from becoming abandoned, Applicant(s) hereby petition for such extensions. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-75900/RDR.

Also enclosed herewith are the following items:

☒ Return Receipt Postcard

Respectfully submitted,



Rory D. Rankin
Reg. No. 47,884
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin,
Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8800

Date: October 13, 2006